VEILLE STRATÉGIQUE

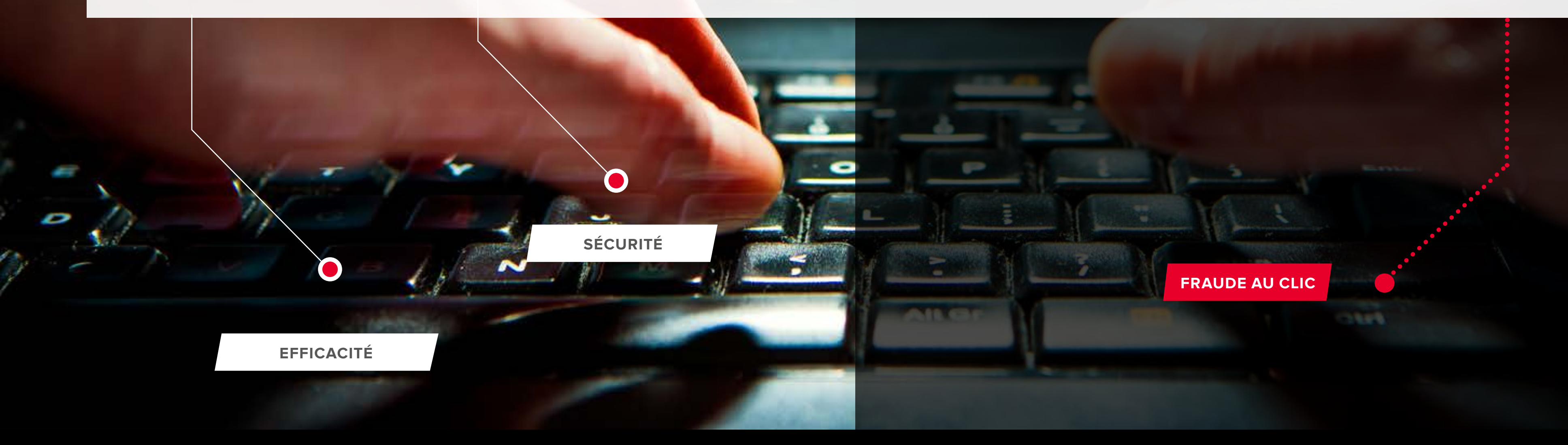
SCANNEURS ET BOTS

NAVIGATEURS SANS TÊTE

PRIORITÉ À LA SÉCURITÉ DES APPLICATIONS

LE RETOUR SUR INVESTISSEMENT MASQUÉ

D’UNE SÉCURITÉ AXÉE SUR LE CLOUD









INTRODUCTION

On vous a peut-être déjà dit que les entreprises de toutes tailles font l'objet d'une transformation numérique, transférant leurs applications et services dans le cloud en vue d'augmenter leur productivité et de booster l'innovation.

Tous les jours, il semble y avoir un nouvel article abordant des sujets comme l'Internet des objets, les données analytiques du Big Data et les architectures cloud et leur potentiel illimité pour les entreprises qui essaient d'obtenir un avantage concurrentiel dans l'univers numérique. Si votre entreprise est en pleine transformation numérique (et c'est très certainement le cas), vous commencez probablement déjà à profiter de certains avantages du cloud public : économies d'échelle, solutions préconfigurées pouvant être lancées en quelques clics, facturation des services utilisés, et bien plus encore. En revanche, on ne vous a certainement pas expliqué comment le modèle de sécurité partagée du cloud public affecte vos responsabilités en matière de sécurité et comment l'utiliser à votre avantage dans un environnement multi-cloud.

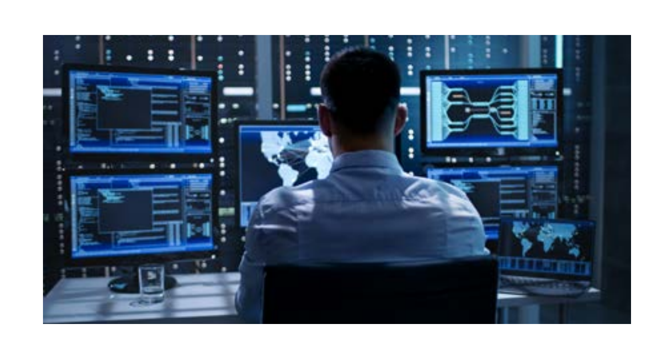
Alors que les fournisseurs cloud gèrent généralement très bien la sécurité des datacenters, infrastructures et systèmes physiques qu'ils vous louent, ils ne peuvent guère vous conseiller sur les éléments que vous développez, déployez ou transférez dans le cloud : à savoir, vos applications, vos services et vos données. Selon une étude de F5 Labs, 53 % des violations de données ciblent initialement la couche applicative[1]. Il s'agit d'une information importante, sachant que tout titulaire d'une carte de crédit peut commencer à utiliser des services cloud pour stocker ou gérer ses données, qu'il en comprenne ou non les implications en termes de sécurité[2]. Quel que soit l'angle sous lequel vous abordez la question, la sécurité dans le cloud est tout aussi importante que celle des datacenters traditionnels.

La nature complexe de ces environnements, la spécificité des architectures et la diversité des contrôles de sécurité exigent que vous adoptiez une approche mesurée pour protéger vos ressources dans le cloud. Une stratégie de sécurité proactive dans le cloud peut vraiment vous aider à optimiser vos processus opérationnels et avoir un impact positif sur vos résultats financiers, et c'est une bonne nouvelle. De plus, il existe une multitude de fournisseurs de solutions de sécurité avec des offres cloud qui vous permettent d'accélérer vos processus de développement, tout en continuant à fournir la sécurité et les services que vos clients attendent.

[1] https://f5.com/labs/articles/threat-intelligence/cyber-security/lessons-learned-from-a-decade-of-data-breaches
[2] https://www.theregister.co.uk/2017/10/10/accenture_amazon_aws_s3/

53 %

SELON UNE ÉTUDE DE F5 LABS, 53 % DES VIOLATIONS DE DONNÉES CIBLENT INITIALEMENT LA COUCHE APPLICATIVE[1].





LES SOLUTIONS DE SÉCURITÉ CLOUD **PEUVENT ÊTRE RAPIDEMENT RENTABLES**

Les réseaux des fournisseurs cloud sont bien cartographiés et consignés, ce qui signifie que des bots et des scanneurs automatisés représentent une part importante du trafic pour les applications cloud. Si le montant de votre facture est calculé en fonction de votre utilisation, vous devez alors prendre en charge des coûts réels et quantifiables chaque fois qu'un bot envoie une demande sur une ressource associée à votre compte cloud. Vous êtes donc vraisemblablement déjà en train de payer des factures salées à cause de ce trafic automatisé. Cependant, en déployant de bons outils de sécurité, tels qu'un ADC (contrôleur de diffusion d'applications) et un pare-feu pour les applications Web (WAF) en amont de vos applications cloud, vous pouvez non seulement les protéger, mais également filtrer le trafic indésirable et réduire les ressources allouées pour honorer inutilement les demandes des bots et des scanneurs. Contrairement aux méthodes de sécurité déployées traditionnellement sur site, vous pouvez bénéficier d'un retour sur investissement quantifiable en utilisant un ADC ou un WAF dans le cloud, tout en garantissant la disponibilité et la sécurité de vos services.

WAF

10 À 40 %

LES BOTS VOUS COÛTENT CHER. JUSQU'À 40 % DU TRAFIC PEUT PROVENIR DE BOTS INDÉSIRABLES, LOGICIELS MALVEILLANTS, SCANNEURS, ETC.

app

UN WAF OU UN ADC PEUVENT ÉLIMINER LE TRAFIC INDÉSIRABLE, TOUT EN RÉDUISANT LE COÛT DE VOS RESSOURCES SUR LE CLOUD.

MISE EN APPLICATION DES PROCESSUS

DEMANDES INCORRECTES

SCANNEURS ET BOTS

LOGICIELS MALVEILLANTS ET FRAUDE

EXTRACTION DE CONTENU

UN WAF PEUT RÉDUIRE LES COÛTS SUR LE CLOUD

En déployant un pare-feu pour les applications Web (WAF) en amont de vos applications cloud, vous pouvez non seulement les protéger, mais également filtrer le trafic indésirable et coûteux, ce qui permet de rentabiliser votre investissement.



LES SOLUTIONS DE SÉCURITÉ CLOUD **PEUVENT STIMULER LA VEILLE STRATÉGIQUE**

Les outils de sécurité peuvent également mieux informer et favoriser la veille stratégique. Un bon WAF ou ADC peut faciliter l'analyse des données et des tendances du trafic en provenance et en direction de vos applications Web reposant sur le cloud. Avec ces renseignements dans la poche, vous pouvez à présent prendre de meilleures décisions sur la gestion des ressources, qui sont susceptibles de réduire vos coûts, tout en répondant aux demandes de vos vrais clients.

La disponibilité est un élément fondamental pour la sécurité des applications. En effet, si votre application n'est pas disponible pour vos clients, il n'y a rien à sécuriser ! En exploitant la technologie ADC dans le cloud, vous pouvez non seulement garantir un haut niveau de disponibilité, mais aussi simplifier les architectures de plus en plus complexes et profiter au maximum d'une stratégie multi-cloud robuste. Un bon partenaire doit être capable de vous fournir à la fois un ADC et des services de sécurité uniformément et sans encombre entre les clouds publics et privés. Il peut aussi vous offrir une gestion et une optimisation adaptées du trafic, de la manière la plus rentable qui soit.

WAF

AVEC UNE VEILLE STRATÉGIQUE PRÉCISE, VOUS ÊTES MIEUX ARMÉ POUR PRENDRE DES DÉCISIONS VRAIMENT AXÉES SUR VOS CLIENTS ET SUSCEPTIBLES DE RÉDUIRE LES COÛTS, TOUT EN RÉPONDANT AUX DEMANDES DE VOS VRAIS CLIENTS.

app

NAVIGATEURS SANS TÊTE

FRAUDE AU CLIC

SCANNEURS ET BOTS

TRANSACTIONS FRAUDULEUSES

ANALYSE DU COMPORTEMENT

NE PRENEZ PAS DE DÉCISIONS COMMERCIALES SANS LES INFORMATIONS NÉCESSAIRES

Avec un pare-feu pour les applications Web (WAF), vous pouvez réduire le trafic malveillant, honorer uniquement les demandes des clients réels et potentiels, et enfin obtenir les informations basées sur les données dont votre entreprise a besoin.



PROFITEZ DES AVANTAGES **D'UNE SÉCURITÉ AXÉE SUR LE DÉVELOPPEMENT**

Même si la sécurité doit être l'affaire de tous, les propriétaires et développeurs d'applications n'ont pas toujours besoin de connaître en détail les règles des WAF, les stratégies de limitation des risques d'attaques DDoS sur la couche 7 ou les protections contre la fraude en ligne. Ils doivent seulement être assurés de la confidentialité, de l'intégrité et de la disponibilité des données en aval de leurs applications. Tout comme il est souvent plus facile et efficace d'utiliser des bibliothèques de code pré-intégrées et des outils tiers, il peut s'avérer judicieux d'exploiter des solutions et services de sécurité avancés pour gagner du temps et réduire les efforts lors du développement. Dans cette optique, une stratégie de sécurité efficace et raisonnable peut facilement être héritée et gérée par ceux qui en comprennent le mieux les enjeux : les pros de la sécurité.

Toutefois, pour que la sécurité joue un rôle de catalyseur commercial, elle doit être fiable et facile à gérer. Elle doit également être intégrée dans les processus de développement tout comme dans les méthodes des développeurs. Ainsi, une stratégie raisonnable qui ne surcharge pas les propriétaires d'applications rencontrera moins de résistance de la part des équipes de développeurs qui doivent agir rapidement. Il s'agit d'un point essentiel à prendre en compte, car si la stratégie entrave le développement au lieu de l'encourager, les équipes de développement n'ont plus qu'à sortir une carte bancaire et envoyer l'application dans le cloud public par eux-mêmes. Notez que c'est une approche qui peut parfois être tentante lorsque vous essayez de respecter des délais ambitieux et d'avoir une flexibilité compétitive.

50 %

LE SHADOW IT REPRÉSENTE ACTUELLEMENT JUSQU'À 50 % DES DÉPENSES DANS DE GRANDES ORGANISATIONS[3].

Il est également important de laisser les propriétaires et développeurs d'applications interagir avec les solutions de sécurité et ADC comme à leur habitude, c'est-à-dire : via des API, des modèles, une infrastructure en tant que code (IaC). Assurez-vous que les solutions que vous déployez dans le cloud reposent sur une API REST performante. Vous devez en effet favoriser l'agilité automatisée dont les propriétaires d'applications et équipes DevOps ont envie et ont besoin. Leur collaboration et leur soutien sont essentiels à la réussite de tout programme de sécurité stratégique.

[3] https://www.cio.com/article/3188726/it-industry/how-to-eliminate-enterprise-shadow-it.html







DES CYCLES DE DÉVELOPPEMENT RAPIDES **NÉCESSITENT DE PUISSANTS OUTILS DE SÉCURITÉ**

Même avec des stratégies de sécurité en place, la protection des applications web est difficile, coûteuse et fastidieuse. Les zones à risque comme les injections indirectes de code à distance (XSS) ou les injections SQL sont bien comprises, mais restent omniprésentes, car il est difficile d'appliquer systématiquement des défenses dédiées pour chaque nouvelle application distribuée. En outre, l'expertise nécessaire pour garantir des pratiques de codage sécurisées et une protection complète contre les risques s'avère de plus en plus difficile à trouver dans les équipes de développement. Selon le rapport 2017 de WhiteHat Security sur la sécurité des applications, la plupart des applications possèdent au moins trois vulnérabilités (et près de 50 % d'entre elles sont critiques). Cela signifie un risque accru de pertes de données, de vols ou de dénis de service si rien n'est corrigé immédiatement[4].

Même si la protection des applications est aujourd'hui de plus en plus difficile à mettre en place, des outils comme les WAF basés sur le cloud peuvent vous aider. Les équipes de développement peuvent exploiter les fonctionnalités d'un WAF performant pour corriger les zones à risque du Top 10 OWASP, atténuer les attaques DoS de la couche 7, détecter et gérer l'activité des bots et déjouer les attaques de type Zero Day, le tout en dehors des cycles normaux de développement pour ne pas les interrompre. L'analyse du comportement peut également s'avérer très efficace pour identifier des tendances et gérer le trafic à destination et en provenance de vos applications web reposant sur le cloud. Et bien que ces fonctionnalités puissent être difficiles à développer et à gérer par vous-même, notez qu'un fournisseur fiable de solutions de sécurité pourra simplifier et améliorer la mise en place de ces services.

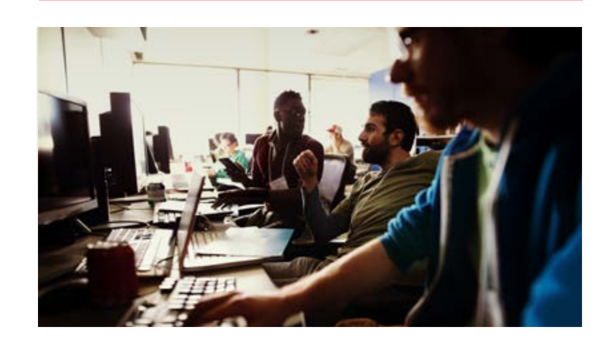
Enfin, puisque 81 % des piratages sont dus à des mots de passe faibles ou volés, la gestion des identités doit être la base fondamentale de toute stratégie de sécurité des applications[5]. En utilisant des identités fédérées ou l'authentification unique (SSO), vous pouvez soulager vos équipes de développement (moins de codage, de vérification et de maintien de l'infrastructure d'authentification), tout en facilitant la vie des utilisateurs qui n'ont aucune envie de gérer un nouveau nom d'utilisateur et mot de passe, même si votre application paraît révolutionnaire.

[4] https://info.whitehatsec.com/rs/675-YBI-674/images/WHS%202017%20Application%20Security%20Report%20FINAL.pdf

[5] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/



LA PLUPART DES APPLICATIONS POSSÈDENT AU MOINS TROIS VULNÉRABILITÉS[4].





RENFORCEZ L'AGILITÉ CLOUD

AVEC UN PARTENAIRE DE CONFIANCE

Les fournisseurs cloud essaient constamment de trouver de nouveaux clients en introduisant toujours plus de services et outils diversifiés à destination des équipes de développement. Si un fournisseur offre un stockage d'archives à long terme bon marché tandis qu'un autre propose une expérience de streaming vidéo améliorée, il paraît judicieux de voir chaque application exploiter les offres de différentes plates-formes cloud. Les stratégies de sécurité portables vous apportent plus de souplesse pour transférer des infrastructures entre différents fournisseurs cloud. Vous accédez ainsi aux fonctions que vous désirez, tout en réalisant des économies. Un ADC portable et avancé peut favoriser une gestion et une distribution fluides des charges, indispensables pour profiter de ces scénarios de déploiement multi-cloud de plus en plus fréquents.

N'oubliez pas que les fournisseurs cloud conçoivent leurs systèmes pour répondre aux besoins du plus grand nombre de clients possible. Cela signifie que l'architecture et les processus proposés ne sont pas toujours parfaitement adaptés à vos besoins spécifiques. C'est à vous d'optimiser toutes les plates-formes cloud pour votre entreprise, et c'est à ce moment-là qu'un fournisseur tiers de confiance peut vous aider à trouver une solution.

Pour tout déploiement d'une application, avec une sécurité uniformisée, dans n'importe quel environnement, vous devrez vous assurer que vos solutions de sécurité sont prêtes pour le multi-cloud, et sont hautement programmables et dirigées par des API. En vous servant de l'expertise d'un partenaire tiers, vous bénéficierez de la portabilité et de la commodité liées au fait d'avoir des services de sécurité uniformes sur l'ensemble des applications, sans devoir gérer des outils propriétaires propres à chaque environnement cloud.





DES SOLUTIONS RAISONNABLES POUR **DES PROGRAMMES DE SÉCURITÉ MULTI-CLOUD**

Au cours d'une enquête réalisée en 2016, près de 75 % des directeurs financiers dans le secteur des technologies ont déclaré que la programmation cloud devrait avoir le plus fort impact mesurable sur leur entreprise à l'avenir[6]. Pour aider votre entreprise à profiter au maximum du cloud, vous aurez besoin d'une stratégie pour contrôler les accès et les identités, préserver la disponibilité de vos services critiques et gérer les vulnérabilités dans les parties de l'infrastructure cloud qui sont sous votre contrôle.

Il sera de plus en plus critique de renforcer la sécurité dans le cloud. D'ici 2021, la cybercriminalité pourrait coûter aux entreprises 6 billions de dollars par an, soit le plus grand transfert de richesse économique de l'histoire, illicite ou non[7]. Beaucoup d'utilisateurs ne s'attendent pas à devenir victimes d'un piratage un jour, pourtant comme La Rochefoucauld le disait déjà au XVIIe siècle : « Ceux qui sont incapables de commettre de grands crimes n'en soupçonnent pas facilement les autres »[8]. En effet, même si vous pensez que personne ne vous ciblera, les hackers sont eux parfaitement prêts à exploiter le climat de confiance instauré par les chefs d'entreprise et propriétaires d'applications. Malheureusement, beaucoup d'entre eux finissent un jour ou l'autre dans la ligne de mire.

Non seulement des outils performants vous permettront de réduire vos coûts, mais ils pourront également vous fournir le niveau de protection adapté pour garantir le bon fonctionnement et la réussite de toutes les applications cloud. En conclusion, méfiez-vous du faux sentiment de sécurité. Choisissez toujours une approche proactive pour protéger vos applications dans les « parties sauvages » de l'univers multi-cloud.

Pour en savoir plus sur la protection des applications, rendez-vous sur f5.com/security.

[6] https://www.bdo.com/getattachment/022227f4-aa2e-4a8b-9739-b0ad6b855415/attachment.aspx?2017-Technology-Outlook-Report_2-17.p
[7] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[8] https://books.google.com/books?id=D5B2BelDhOQC&printsec=frontcover#v=onepage&q&f=false

PRIORITÉ À LA SÉCURITÉ DES APPLICATIONS

Les applications toujours activées et toujours connectées peuvent dynamiser et transformer votre entreprise. Cependant, elles peuvent également servir de portes d'entrée vers vos données malgré les protections de vos pare-feu. Puisque la plupart des attaques surviennent au niveau des applications, la protection des fonctionnalités qui dynamisent votre entreprise implique forcément la protection des applications qui leur permettent d'exister.

